

PURPOSE

Computer systems and the environments in which they operate change continually. Unauthorized changes in an operational system or environment create an unstable configuration baseline that can introduce vulnerabilities that could negatively impact the security posture of the information resource.

The purpose of change management in an information security infrastructure is to manage the effects of changes or differences in configurations on an information system or network (including hardware, software and infrastructure). Change management allows system owners to handle changes in a controlled, predictable and repeatable manner and assess, identify and minimize the risks to operations and security prior to implementation.

POLICY

State of Georgia information systems, in the operations phase of the system lifecycle, shall have formal change control procedures that adequately consider the potential security impacts of the change to the information system or its surrounding environment.

System Owners shall establish formal change management procedures that include a process to document, review, approve, and monitor all changes to operational computing and communications infrastructure and assess the risks, impacts and benefits of the change.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Operational Change Control (SS-08-026)

REFERENCES

NIST SP 800-100 Information Security Handbook for Managers (Ch 14)

NIST Special Publication 800-160 vol. <https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final>

TERMS and DEFINITIONS

Change Management is the process of controlling modifications to hardware, software and infrastructure to ensure that information resources are protected against improper modification and reduce the risks to system operations and security before, during and after system implementation.